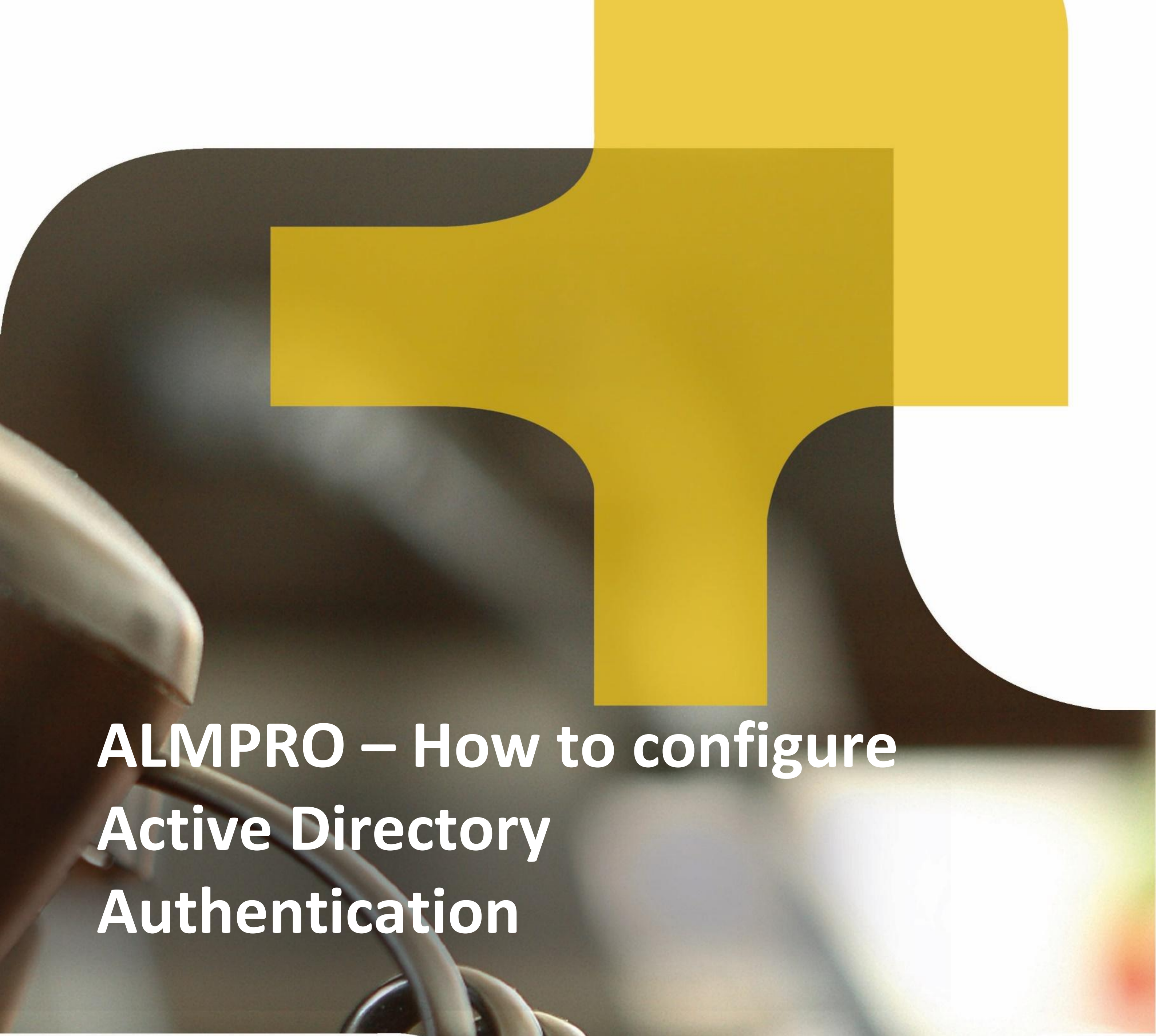


ALMPRO – How to configure Active Directory Authentication

RSconnect
IPT Security

Oude Oeverstraat 120-4
6811 JZ
Arnhem
The Netherlands

t: +31(0) 88 1221 800
f: +31(0) 88 1221 899
www.rsconnect.net
info@rsconnect.net

How to configure Active Directory Authentication within ALMPRO

This How-To guide explains how to configure Active Directory in ALMPRO.

The default behaviour of ALMPRO is that it prompts the user for its Extension Mobility user name and PIN at first use.

However, if your CallManager is configured to accept the Windows login name as the userid, then ALMPRO can automatically login the user's phone without the need to enter a username or PIN.
This document applies to ALMPRO.

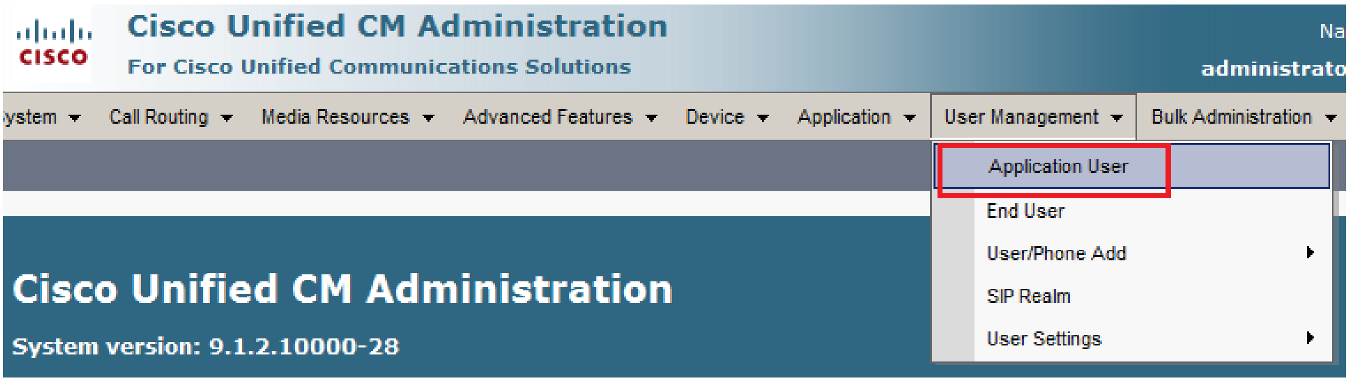
To support lower versions, please contact support@rsconnect.net

Required CUCM configuration

The First step is to configure one generic Application User in CUCM with permissions to 3rd party applications (ALM) to login Extension Mobility:

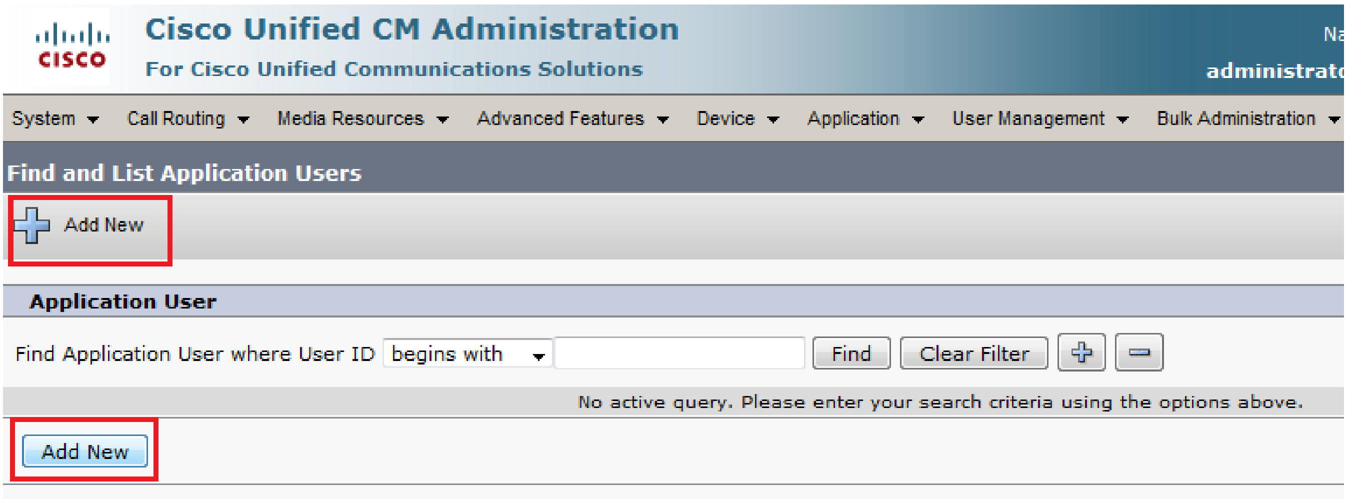
a) Login to the CCM admin page

b) Open User Management/Application User



System version: 9.1.2.10000-28

c) Click Add new user



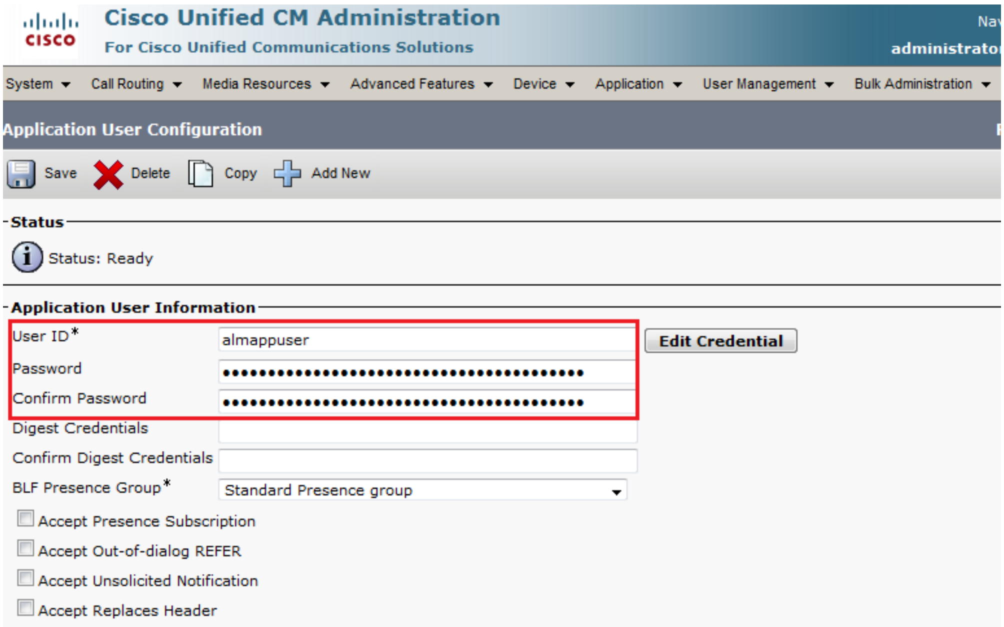
Find Application User where User ID begins with

No active query. Please enter your search criteria using the options above.

d) Create a User ID and an App Password and add the user to the "Standard EM Authentication Proxy rights" group. Remember the chosen user ID and App password for step 2.

Application Username	almappuser*
Application Password	

* example



Cisco Unified CM Administration
For Cisco Unified Communications Solutions

Application User Configuration

Status

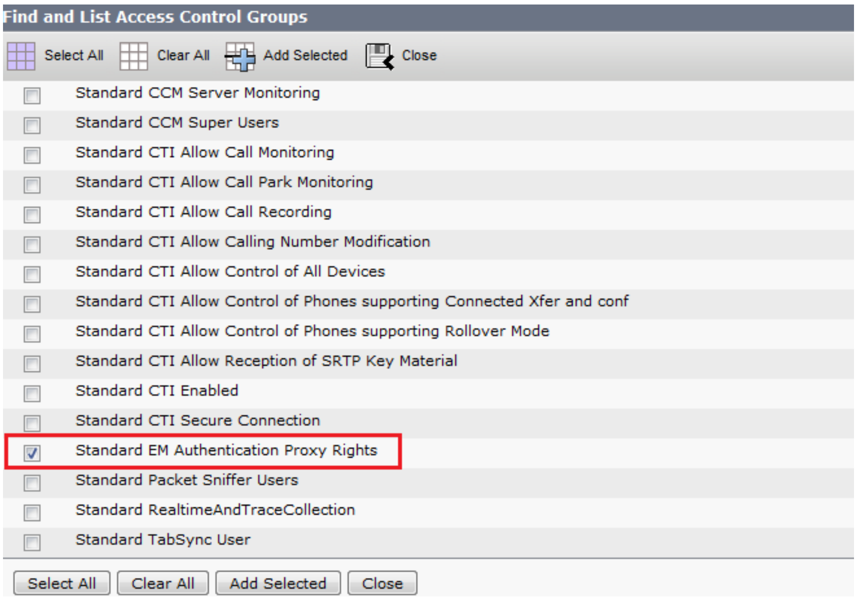
Status: Ready

Application User Information

User ID*	almappuser
Password	••
Confirm Password	••
Digest Credentials	
Confirm Digest Credentials	
BLF Presence Group*	Standard Presence group

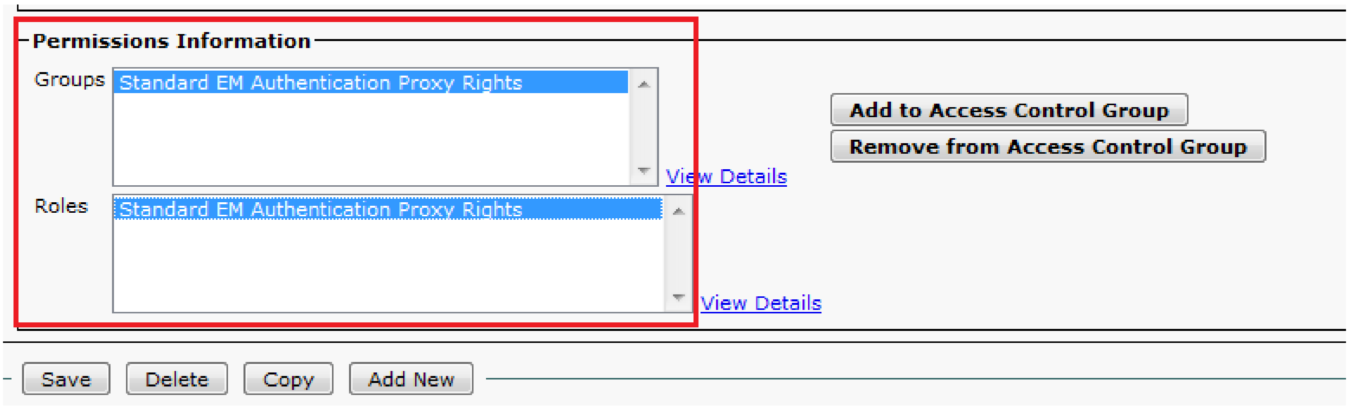
☐ Accept Presence Subscription
☐ Accept Out-of-dialog REFER
☐ Accept Unsolicited Notification
☐ Accept Replaces Header

e) Add the AppUser to the “Standard EM Authentication Proxy Rights” Access Control Group



Find and List Access Control Groups

☐ Standard CCM Server Monitoring
☐ Standard CCM Super Users
☐ Standard CTI Allow Call Monitoring
☐ Standard CTI Allow Call Park Monitoring
☐ Standard CTI Allow Call Recording
☐ Standard CTI Allow Calling Number Modification
☐ Standard CTI Allow Control of All Devices
☐ Standard CTI Allow Control of Phones supporting Connected Xfer and conf
☐ Standard CTI Allow Control of Phones supporting Rollover Mode
☐ Standard CTI Allow Reception of SRTP Key Material
☐ Standard CTI Enabled
☐ Standard CTI Secure Connection
☑ Standard EM Authentication Proxy Rights
☐ Standard Packet Sniffer Users
☐ Standard RealtimeAndTraceCollection
☐ Standard TabSync User



Permissions Information

Groups	Standard EM Authentication Proxy Rights
Roles	Standard EM Authentication Proxy Rights

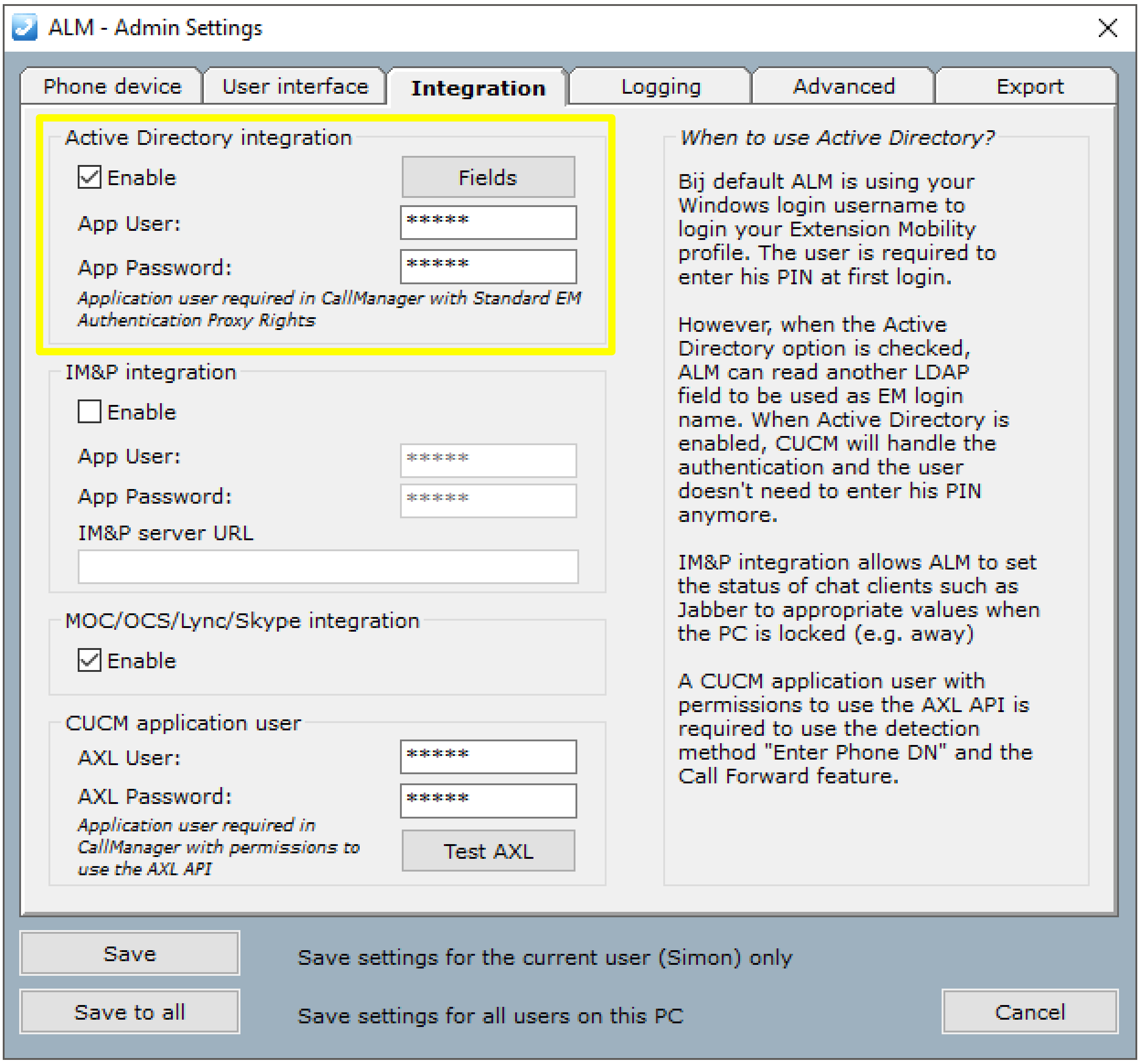
The second step is to configure the ALMPRO client to user the created App user from step 1.

a) Open ALMPRO (double click ALMPRO icon in the system tray)

b) Click on Options/Admin settings (If this option is disabled, then make sure you run ALMPRO as administrator, even if you already have administrator permissions.

c) Open the Integration TAB

d) Enable Active Directory Integration and enter the app user ID and app password created in step 1d



ALM - Admin Settings

Active Directory integration

☑ Enable

App User: *****

App Password: *****

Application user required in CallManager with Standard EM Authentication Proxy Rights

IM&P integration

☐ Enable

App User: *****

App Password: *****

IM&P server URL

MOC/OCS/Lync/Skype integration

☑ Enable

CUCM application user

AXL User: *****

AXL Password: *****

Application user required in CallManager with permissions to use the AXL API

When to use Active Directory?

Bij default ALM is using your Windows login username to login your Extension Mobility profile. The user is required to enter his PIN at first login.

However, when the Active Directory option is checked, ALM can read another LDAP field to be used as EM login name. When Active Directory is enabled, CUCM will handle the authentication and the user doesn't need to enter his PIN anymore.

IM&P integration allows ALM to set the status of chat clients such as Jabber to appropriate values when the PC is locked (e.g. away)

A CUCM application user with permissions to use the AXL API is required to use the detection method "Enter Phone DN" and the Call Forward feature.

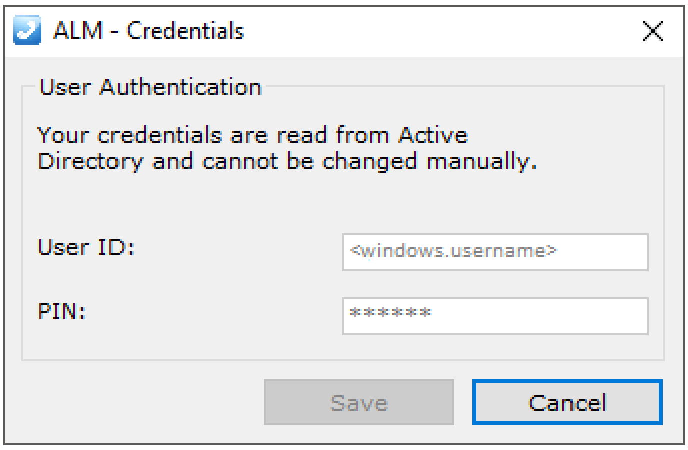
Save settings for the current user (Simon) only

Save settings for all users on this PC

e) Click Save

f) Within ALMPRO click on Options/Change credentials

g) It should display your Windows login name and disabled PIN and Save button as listed below:



ALM - Credentials

User Authentication

Your credentials are read from Active Directory and cannot be changed manually.

User ID: <windows.username>

PIN: ******

Ordering Information

Please send your quotation requests to sales@rsconnect.net along with the number of licenses you require.

1 license is required for 1 PC/Phone combination, the license is not user or phone based.
If two employees use 1 computer in combination with 1 IP Phone you will require 1 license.

Additional Information

For any additional information please contact or visit:

- United Kingdom: +44 203 608 8259
- Other countries: +31 88 1221 800
- http://www.rsconnect.net
- sales@rsconnect.net